Le choix d'un prestataire Cloud

Le choix du prestataire Cloud est important pour votre projet IA. Si la sélection du Prestataire et du produit est naturellement prise sur des critères technologiques, tarifaires ou encore humains. Il est capital de prendre en considération la réglementation et les problématiques juridiques sous-jacentes applicables à votre projet.

Si, de manière naturelle, une lecture attentive des documents contractuels visera à vous rassurer quant aux questions de :

- Niveaux de service et engagements contractuels
- Responsabilité contractuelle et clauses limitatives de responsabilité
- Tarification
- Garantie
- Droit applicable /Juridictions compétentes

Il existe tout un ensemble de risques juridiques susceptibles de vous concerner et pour lesquels les réponses s'avèrent beaucoup plus difficiles à trouver auprès de votre prestataire de Cloud.

1. La conformité au RGPD doit guider le choix

Dès lors que vous traitez des données à caractère personnel de citoyens européens[1], vous êtes soumis au Règlement Général sur la Protection des Données (RGPD)[2] et devez prendre en compte l'ensemble des obligations vous incombant en votre qualité de Responsable de traitement[3].

Le choix de votre prestataire Cloud, qui interviendra en qualité de sous-traitant, sera par conséquent déterminant dans votre capacité à respecter vos propres obligations réglementaires.

Si les données utilisées dans le cadre du projet d'IA sont anonymes (ne pas confondre anonymisation et pseudonymisation, aucune ré-identification ne doit être possible), le RGPD ne s'appliquera pas.

OÙ SONT LOCALISÉES VOS DONNÉES ?

La localisation des infrastructures d'hébergement est un élément important.

Si vos données ne sont pas localisées sur le territoire Français ou sur le territoire de l'Union Européenne (ci-après "UE"), on parlera juridiquement d'un transfert de données vers un pays étranger.

Une telle opération ne devrait être envisagée que si le pays destinataire présente un niveau de protection adéquat et/ou si elle est strictement encadrée via des mécanismes juridiques spécifiques (Clauses contractuelles types (ou "CCT") de la Commission européenne)[4].

Il est d'usage, pour les prestataires Cloud, de communiquer une zone géographique d'hébergement qui peut couvrir différents pays (ex: Europe).

Toutefois, il est important de vérifier la liste des sous-traitants de ce Prestataire et la finalité de traitement de vos données par ces derniers ainsi que la localisation précise des données pour l'ensemble des services souscrits (ex: support).

Par ailleurs, il est recommandé la mise en place de sauvegardes régulières qui peuvent être réalisées sur différents pays pour éviter tout risque de perte de données mais exposent aussi vos données à différentes réglementations et menaces.

QUI ACCÈDE À VOS DONNÉES ?

Il est important de rappeler qu'un transfert de données hors UE peut également intervenir dès lors que des données, même localisées sur le territoire de l'UE, sont accessibles par des personnes situées en dehors du territoire de l'UE.

En effet, dans l'hypothèse d'un prestataire Cloud dont les équipes chargées de l'administration ou de la maintenance de votre offre Cloud seraient localisées en dehors de l'UE, et si ces équipes disposent d'un accès aux données à caractère personnel stockées sur votre offre Cloud, alors cela s'apparentera à un transfert de données hors UE et vous devrez respecter les procédures et mécanismes juridiques énoncés précédemment.

N'OUBLIEZ PAS D'INFORMER LES PERSONNES CONCERNÉES AVANT TOUT TRANSFERT EN DEHORS DE L'UE

Dans les deux cas énoncés précédemment, localisation des données en dehors de l'UE ou accès depuis un pays hors de l'UE, le RGPD prévoit que le responsable de traitement doit informer, avant tout transfert de données, les personnes dont les données à caractère personnel seraient ainsi transférées hors de l'UE.

PAS DE DIFFICULTÉ À CHOISIR UN PRESTATAIRE CLOUD US ?

Bien conscientes des enjeux liés aux transferts de données hors de l'UE et notamment vers les USA dont sont originaires la majorité des acteurs majeurs du Cloud, les autorités européennes et américaines se sont efforcées de construire, au cours des dernières années, un cadre juridique satisfaisant.

Récemment, par décision du 10 juillet 2023, la Commission européenne a estimé que les États-Unis assuraient désormais un niveau de protection des données personnelles équivalent à celui de l'Union européenne.

Cette décision met fin, pour le moment, à une période d'incertitude depuis l'arrêt de la CJUE du 16 juillet 2020 (dit « Schrems II »[5]) qui avait annulé la décision d'adéquation de la Commission européenne validant le Privacy Shield.

Désormais, si le siège social du Prestataire Cloud est situé aux USA :

- Cas 1 : L'éditeur figure sur la liste mise à disposition sur le site du Département du Commerce des États-Unis. (ici) => pas de CCT à signer
- Cas 2 : S'il ne figure pas sur cette liste => CCT à signer

Le recours à un prestataire Cloud non européen peut complexifier votre capacité à vous conformer au RGPD dès lors que le cadre réglementaire est mouvant.

2. La problématique des demandes judiciaires

Dans l'hypothèse où vous-même ou l'un de vos clients / utilisateurs feriez l'objet d'une enquête judiciaire, une demande de copie ou de saisie de vos données pourrait être adressée à votre prestataire Cloud.

Celui-ci procédera à l'analyse juridique de la demande et, si sa légalité ne peut pas être contestée, il sera tenu de l'exécuter.

Votre prestataire, s'il dispose de la capacité de procéder à cette copie de données (accès à un outil de gestion ou d'administration dans le cadre d'un cloud public, administration des espaces de stockage ou de sauvegarde), sera tenu de procéder à ces opérations.

Une demande de copie ou une saisie de données est traditionnellement soumise au secret judiciaire, ce qui interdit à votre prestataire Cloud de vous communiquer l'existence de cette demande mais également ses caractéristiques : autorité requérante, qualification pénale, périmètre de la demande.

La localisation des données d'un service Cloud détermine le droit applicable sur ces données et donc les autorités judiciaires en capacité de les requérir.

Dans l'hypothèse d'une demande des autorités judiciaires sur vos données, il est important que vous soyez en mesure de connaître le système judiciaire de ce pays mais également les procédures judiciaires et extrajudiciaires qui vous permettront de défendre au mieux vos intérêts.

Au-delà des seules demandes judiciaires, cette problématique peut également intervenir dans le cadre de litiges commerciaux, concurrence, etc. Une demande de saisie-contrefaçon par exemple pourrait être adressée à votre prestataire cloud et vous obliger à engager toute voie de recours susceptible de garantir vos droits.

Il est enfin rappelé que, si le chiffrement peut permettre d'éviter un accès aux données, il n'est pas garanti que cela suffise à dissuader la réalisation de ces opérations de copie par des services de police ou agences de renseignement.

MES DONNÉES SONT EN UE, DONC PROTÉGÉES DE TOUTE INGÉRENCE ÉTRANGÈRE ?

Selon les pays, la réglementation permettant l'accès aux données par les services de Police ou de renseignement peut prévoir la possibilité de requérir l'accès à des données localisées en dehors du territoire national. On parle alors d'extraterritorialité.

Les USA disposent de plusieurs réglementations comme les PATRIOT et CLOUD Acts qui permettent ainsi aux services de renseignement américains de solliciter, auprès des prestataires Cloud, la communication des données localisées en dehors du territoire américain dès lors que ces prestataires disposent d'un accès à ces données. Il appartient alors au prestataire Cloud américain de s'opposer auprès des autorités américaines à la communication de ces données.

COMMENT SE PRÉMUNIR DE CE RISQUE ?

L'Agence Nationale de la sécurité des systèmes d'information (ANSSI) bien consciente de ces enjeux a élaboré le référentiel SecNumCloud[1] qui permet la qualification de prestataires cloud répondant à un cahier des charges strict visant à apporter des garanties aux utilisateurs publics ou privés quant aux risques d'ingérence étrangère.

La liste de ces prestataires qualifiés est accessible sur le site de l'ANSSI.[2]

[1] https://www.ssi.gouv.fr/actualite/lanssi-actualise-le-referentiel-secnumcloud/
[2] https://www.ssi.gouv.fr/entreprise/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-service-dinformatique-en-nuage-secnumcloud/

Le choix d'un prestataire Cloud

En fonction de la criticité des données hébergées chez le prestataire, il est nécessaire d'évaluer la probabilité de ce type d'ingérence étrangère dans votre secteur et les conséquences financières, organisationnelles, de développement.

Exigez dans vos contrats la communication systématique des demandes d'autorités étrangères et la faculté de s'y opposer.

La dernière question à se poser :
Cherchez-vous un futur partenaire ou un futur concurrent potentiel ?

Les prestataires Cloud peuvent vouloir se positionner sur de multiples marchés et proposer un panel de services et de solutions le plus large possible. On observe ainsi différentes approches qui peuvent se baser sur de multiples partenariats, marketplaces mais également sur des acquisitions. Une telle philosophie peut aboutir à ce que vous soyez un jour en concurrence directe avec votre prestataire Cloud.[1]

Un prestataire Cloud peut indirectement disposer d'un ensemble d'informations permettant de connaître la nature de votre activité :

- Ressources consommées de CPU, RAM
- Flux réseau
- Croissance de votre infrastructure, etc.

Toutes ces informations, indirectement accessibles, peuvent permettre à votre prestataire Cloud de mieux comprendre votre activité et être utilisées à des fins totalement extérieures au service souscrit.

Enfin, cette concurrence peut aussi intervenir en raison d'intérêts supérieurs : enjeux de souveraineté nationale, intelligence économique. La Direction générale de la Sécurité intérieure a ainsi alerté sur l'importance de cette question.[2]

[1] Acquisition d'OpenAI par Microsoft et intégration de Chatgpt au moteur de recherche Bing et au navigateur Internet Edge : https://siecledigital.fr/2023/02/08/microsoft-chatgpt-bing-edge/
[2]https://www.economie.gouv.fr/files/dgsi-special-cybersecurite.pdf